ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 19, Issue 2, 2025

SECURE SHARING OF IDENTITY (KYC)

[1]MR. SK.GOUSE BASHA,[2]YELURI SRAVYA, [3]KATTEBOYINA AKSHAYA SARANYA, [4]SHAIK SAMAN, [5]THUMMA VENKATESH.

[1](ASSISTANT PROFESSOR), [2345]B.TECH STUDENTS
DEPARTMENT OF CSE, RISE KRISHNA SAI PRAKASAM GROUP OF INSTITUTIONS

ABSTRACT

With cloud storage services, users can store their data in the cloud and efficiently access the data at any time and any location. However, when data are stored in the cloud, there is a risk of data loss because users lose direct control over their data. To solve this problem, many cloud storage auditing techniques have been studied. In 2019, Tian *et al.* proposed a public auditing scheme for shared data that supports data privacy, identity traceability, and group dynamics. In this paper, we point out that their scheme is insecure against tag forgery or proof forgery attacks, which means that, even if the cloud server has deleted some outsourced data, it can still generate valid proof that the server had accurately stored the data. We then propose a new

scheme that provides the same functionalities and is secure against the above attacks. Moreover, we compare the results with other schemes in terms of computation and communication costs

1.INTRODUCTION

Cloud storage provides users with significant storage capacity and advantages such as a cost reduction, scalability, and convenient access to the stored data. Therefore, cloud storage that is managed and maintained by professional cloud service providers (CSPs) is widely used by many enterprises and personal clients [1]. Once the data are stored in cloud storage, the clients lose direct control over the stored _les. Despite this, the CSPs must ensure that the client data are placed in cloud storage without any modification or substitution. The simplest way to achieve this is by checking the integrity of the stored data after downloading. When the capacity of the stored data is large, it is quite inefficient, and thus many methods for verifying the integrity of the data stored in the cloud without a full download have been proposed [2]_[34].

These techniques are called cloud storage auditing and can be classified into private auditing and public auditing according to the

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

subject of the integrity verification. In private auditing, verification is achieved by users who have ownership of the stored data. Public auditing is conducted by a third-party auditor (TPA) on behalf of the users to reduce their burden, and thus public auditing schemes are more widely employed for cloud storage auditing. Public auditing schemes provide various properties depending on the environment, such as privacy preservation [5]_[9], data dynamics [10]_[13], and shared data [14]_[33]. Privacy-preserving auditing is used to conduct an integrity verification while protecting data information from the TPA, and dynamic data auditing is where legitimate users are free to add, delete, or change the stored data. Shared data auditing means freely sharing data within a legitimate user group. In this case, a legitimate user group should be defined, and user addition and revocation should be carefully considered. Recently, schemes that satisfy identity traceability, a concept that can trace the abnormal behavior of legitimate users in shared data auditing, have also been propose

Tian et al. [25] proposed a scheme that supports privacy preservation, data dynamics, and identity traceability in shared data auditing. For efficient user enrollment and revocation, the authors adopted the lazy revocation technique. Moreover, to secure the design against collusion attacks between the revoked user and server, they apply a technique in which the group manager manages messages and tag blocks generated by the revoked user to the scheme. Because the lazy-revocation technique is applied to the scheme, even if a user is revoked, no additional operation occurs until additional changes are made to the block.

In this paper, we show that Tian et al.'s scheme [25] is insecure against two types of attacks, a tag forgery and a proof forgery, and proposed a new scheme that provides the same functionality and is secure against the above attacks. In this scheme, a tag forgery is possible by exploiting the vulnerability in which the tag is created in a malleable way, and a proof forgery is possible by exploiting the secret value being exposed to the server when additional changes to the block occur after the user is revoked. In general, the contributions of this study can be summarized as follows

1. We show that Tian et al.'s scheme [25] is insecure against two types of attacks: tag and proof forgeries. In tag forgery, we show that an attacker can create a valid tag for the modified message without knowing any secret values. In the proof forgery, we show that an attacker can create a valid proof for

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

the given challenged message even if some _les stored on the cloud have been deleted.

2. We design a new public auditing scheme that is secure against the above attacks and has the same functionalities, such as privacy preservation, data dynamics, data sharing, and identity traceability. We changed the tag generation method to eliminate the malleable property and the data proof generation method to enhance the privacy preservation. We also changed the lazy revocation process to protect the secret information from the CSP and proposed an active revocation process to flexibly apply the various environments.

3. We formally prove the security of the proposed scheme. According to the theorems, the attacker cannot generate a valid tag and proof without knowing the secret values or the original messages, respectively. We also provide comparison results with other schemes in terms of the computation and communication costs.

The rest of this paper is organized as follows. In Section II, we introduce the background, and in Section III, we review Tian et al.'s scheme [25].We present our detailed scheme for public auditing in Section IV, and provide the security and efficiency of our scheme in Section V. Finally, we conclude this paper in Section VI.

2.LITERATURE SURVEY

Ateniese et al. [6] are the first to consider public auditability in their defined “provable data possession” (PDP) model for ensuring possession of files on untrusted storages. In their scheme, utilize RSA based homomorphic tags for auditing outsourced data, thus public auditability is achieved. However, Ateniese et al. do not consider the case of dynamic data storage, and the direct extension of their scheme from static data storage to dynamic case may suffer design and security problems. In their subsequent work [7], Ateniese et al. propose a dynamic version of the prior PDP scheme. However, the system imposes a priori bound on the number of queries and does not support fully dynamic data operations, i.e., it only allows very basic block operations with limited functionality, and block insertions cannot be supported. In [17], Wang et al. consider dynamic data storage in a distributed scenario, and the proposed challenge-response protocol can both determine the data correctness and locate possible errors. Similar to [7], they only consider partial support for dynamic data operation. Juels et al. [10] describe a “proof of retrievability”

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

(PoR) model, where spot-checking and errorcorrecting codes are used to ensure both "possession" and "retrievability" of data files on archive service systems. Specifically, some special blocks called "sentinels" are randomly embedded into the data file F for detection purpose, and F is further encrypted to protect the positions of these special blocks. However, like [7], the number of queries a client can perform is also a fixed priori, and the introduction of precomputed "sentinels" prevents the development of realizing dynamic data updates. Shacham et al. [16] design an improved PoR scheme with full proofs of security in the security model defined in [10]. They use publicly verifiable homomorphic authenticators built from BLS signatures , based on which the proofs can be aggregated into a small authenticator value, and public retrievability is achieved. Still, the authors only consider static data files. Erway et al. [9] was the first to explore constructions for dynamic provable data possession. They extend the PDP model in [6] to support provable updates to stored data files using rank-based authenticated skip lists. The scheme is essentially a fully dynamic version of the PDP solution. To support updates, especially for block insertion, they eliminate the index information in the "tag" computation in Ateniese"s PDP model [6] and employ authenticated skip list data structure to authenticate the tag information of challenged or updated blocks first before the verification procedure. However, the efficiency of their scheme remains unclear. Shan et al.[13] introduce TPA concept to maintain data integrity and preserve privacy. It reduces online burden and keeps the privacy preserve. Chen et al.[8] gives mechanism for auditing the correctness of data with multiple server. Frenz et al.[11] introduce a new strategy ,an Oblivious out-sourced storage which is based on Oblivious RAM technique. This idea used to conceal user access pattern and preserve the identity. Although the existing schemes aim at providing integrity verification for different data storage systems, the problem of supporting both public auditability and data dynamics has not been fully addressed. How to achieve a secure and efficient design to seamlessly integrate these two important components for data storage service remains an open challenging task in Cloud Computing. Two basic solutions (i.e., the MAC-based and signature based schemes) for realizing data auditability and discuss their demerits in supporting public auditability and data dynamics. Secondly,

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

generalize the support of data dynamics to both proof of retrievability (PoR) and provable data possession (PDP) models and discuss the impact of dynamic data operations on the overall system efficiency both. In particular, emphasize that while dynamic data updates can be performed efficiently in PDP models more efficient protocols need to be designed for the update of the encoded files in PoR models

3.SYSTEM ANALYSIS

Ateniese*et al.* [2] first introduced a provable data possession scheme called PDP and provided two provably secure PDP schemes using RSA-based homomorphic authenticators. This supports public verification with lower communication and computation costs. At the same time, Juels *et al.* [3] first proposed the concept and a formal security model of proof of retrievability (POR) and a sentinel-based POR scheme with certain properties. Later, Shacham*et al.* [4] improved the POR scheme and proposed a new public auditing scheme that was built from the BLS signature [36] and is secure in the random oracle model. In recent years, many studies have been conducted on cloud storage auditing, supporting various functionalities such as data privacy preservation, data dynamics, and shared data.

Erway *et al.* [10] first proposed the PDP scheme using a rank-based authenticated skip list to support data dynamics. However, the scheme suffers from high computational and communication costs, and to address this concern, Wang *et al.* [11] proposed a new auditing scheme employing the Merkle Hash Tree (MHT), which is much simpler.

Although Wang *et al.* [5] proposed a privacy-preserving public auditing scheme, their approach requires heavy communication and computation costs in the audit and data update process. Zhu *et al.* [12] also proposed a new scheme using another authenticated data structure, called an index hash table (IHT), to support data dynamics. Although this scheme succeeded in reducing the communication and computation costs, it did not resolve the inefficient problem of lookup and updating operations. Shen *et al.* [13] proposed a new efficient scheme with a doubly linked information table and location array. Tian *etal.* [25] recently proposed a more efficient scheme using a dynamic hash table (DHT), which has been proven to be more effective than IHT for data updating [12]. In terms of data privacy, Wang *et al.* [5] first proposed a privacy-preserving public auditing scheme

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

to protect data privacy through random masking, and many schemes for predicting data privacy have been studied [6]_[9].

Wang *et al.* [14] proposed an efficient public auditing scheme called Knox for shared data. The scheme supports hiding the identity of individual users based on a group signature, but does not support a user revocation. In Oruta [15], a ring signature is used to hide the identity of individual users; however,the scheme also has a problem in that all user keys and block tags must be regenerated to provide a user revocation.

Wang *et al.* [16] also proposed a scheme that can achieve a user revocation using a proxy re-signature. The scheme utilizes a proxy for a resigning used to update the tag generated by the revoked user; however, it is vulnerable to collusion attacks between an invalid user and the cloud server.

In addition, Jiang *et al.* [17] proposed a new public auditing scheme that combines a vector commitment [37] and a verifier-local-revocation group signature [38]. During the revocation phase, the computational costs are relatively high because it is necessary to first find the tags generated by the revoked user and regenerate them. Yu *et al.* [18], [19] also proposed a new scheme using polynomial authentication tags and proxy re-signatures. Although this scheme can reduce the communication overhead during verification, it can suffer from a collusion attack because the revoked user still has a valid private key and might collude with the CSP.

Disadvantages

- An existing system,the system doesn't have data auditing techniques to find data verification.
- The system doesn't have Dynamic Hash tables to maintain the blocks.

3.1 PROPOSED SYSTEM

1. We show that Tian *et al.*'s scheme [25] is insecure against two types of attacks: tag and proof forgeries. In tag forgery, we show that an attacker can create a valid tag for the modified message without knowing any secret values. In the proof forgery, we show that an attacker can create a valid proof for the given challenged message even if some files stored on the cloud have been deleted.
2. We design a new public auditing scheme that is secure against the above attacks and has the same functionalities, such as privacy preservation, data dynamics, data sharing, and identity traceability. We changed the tag generation method to

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

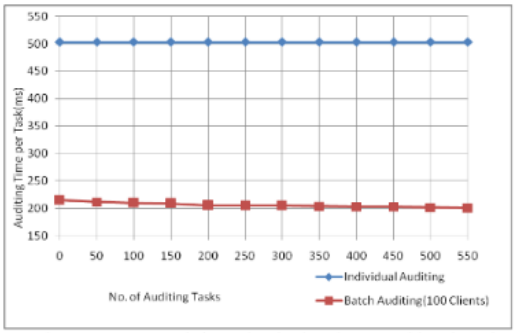
eliminate the malleable property and the data proof generation method to enhance the privacy preservation. We also changed the lazy revocation process to protect the secret information from the CSP and proposed an active revocation process to flexibly apply the various environments.

3. We formally prove the security of the proposed scheme. According to the theorems, the attacker cannot generate a valid tag and proof without knowing the secret values or the original messages, respectively. We also provide comparison results with other schemes in terms of the computation and communication costs.

Advantages

- In the proposed system, to manage the data blocks handled by revoked users, we use an extended dynamic hash table (EDHT).
- In the proposed system, the modification record table (MRT) is a table in which the group manager records operations for each block to provide identity traceability and is a two-dimensional data structure.

4. OUTPUTSCREENS



5. CONCLUSION

Here in this paper, we are given the privacy –preserving public auditing scheme which supports data dynamic operations. Public auditing scheme supports hashing technique. The data dynamic operations can get performed by using Merkle Hash Tree(MHT). We use multiple TPA for the auditing process which handles multiple users through batch auditing. We utilize ring signature for secure cloud storage which ensures that during the auditing process the TPA would not learn any information or knowledge about data content of group stored on cloud server. Ring signature preserves the identity of the signer from the verifier. We use HARS scheme for group of users in which they share data to each other and update and delete data block wise manner.

ISSN 2454-9940

www.ijasem.org

Vol 19, Issue 2, 2025

6. REFERENCE

[1] (Apr. 2021). *Cloud Storage-Global Market Trajectory and Analyt-ics*. [Online]. Available: https://www.researchandmarkets.com/reports/ 5140992/cloud-storage-global-market-trajectory-and

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, ``Provable data possession at untrusted stores," in *Proc. 14th ACM Conf. Comput.Commun.Secur.(CCS)*, 2007, pp. 598_609.

[3] A. Juels and B. S. Kaliski, ``PORs: Proofs of retrievability for large _les," in *Proc. 14th ACM Conf. Comput. Commun.Secur. (CCS)*, Oct. 2007, pp. 584_597.

[4] H. Shacham and B. Waters, ``Compact proofs of retrievability," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Berlin, Germany: Springer, 2008, pp. 90_107.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou,``Privacy-preserving public auditing for data storage security in cloud computing," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1_9.

[6] Z. Hao, S. Zhong, and N. Yu, ``A privacy-preserving remote data integrity checking protocol with data dynamics and public veri_ability," *IEEE Trans. Knowl. Data Eng.*, vol. 23, no. 9, pp. 1432_1437, Sep. 2011.

[7] K. Yang and X. Jia, ``Anef_cient and secure dynamic auditing protocol for data storage in cloud computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 9, pp. 1717_1726, Sep. 2013.